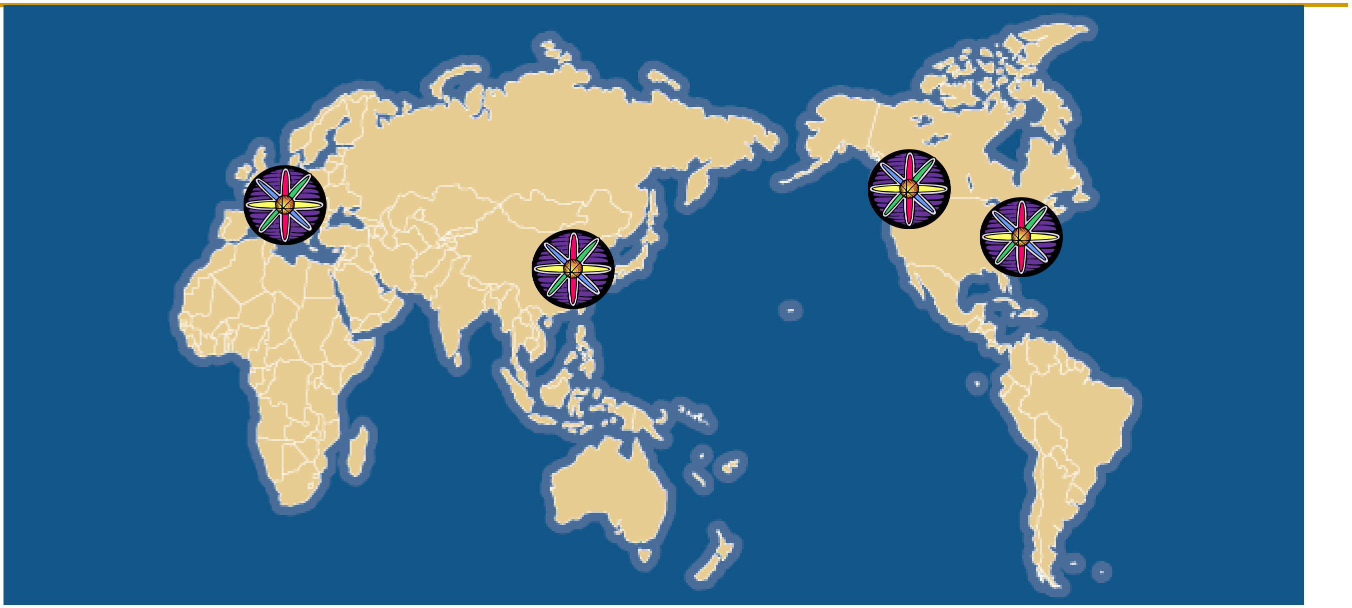
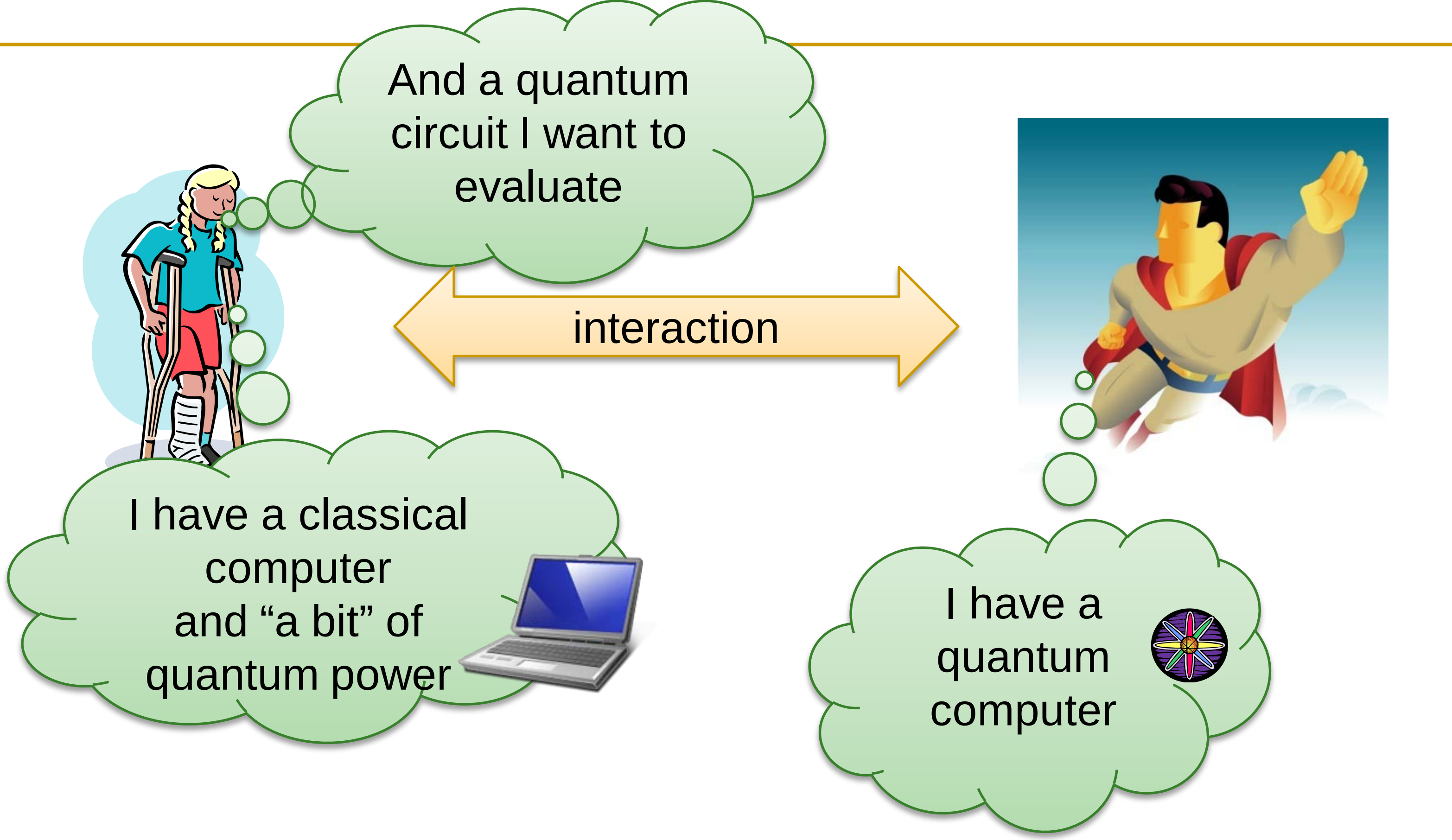
Universal Blind Quantum Computation

Anne Broadbent (Institute for Quantum Computing, University of Waterloo)
with
Joseph Fitzsimons (Oxford)
Elham Kashefi (Edinburgh)

20??



- The year is 20??. A few centers around the world have managed to build quantum computers.
- They allow users to have remote access to their quantum computers.



And a quantum circuit I want to evaluate

interaction

I have a classical computer and “a bit” of quantum power

I have a quantum computer

- How can Alice be convinced that the output provided by the quantum computer is correct?
- Can she do this while keeping her input private?

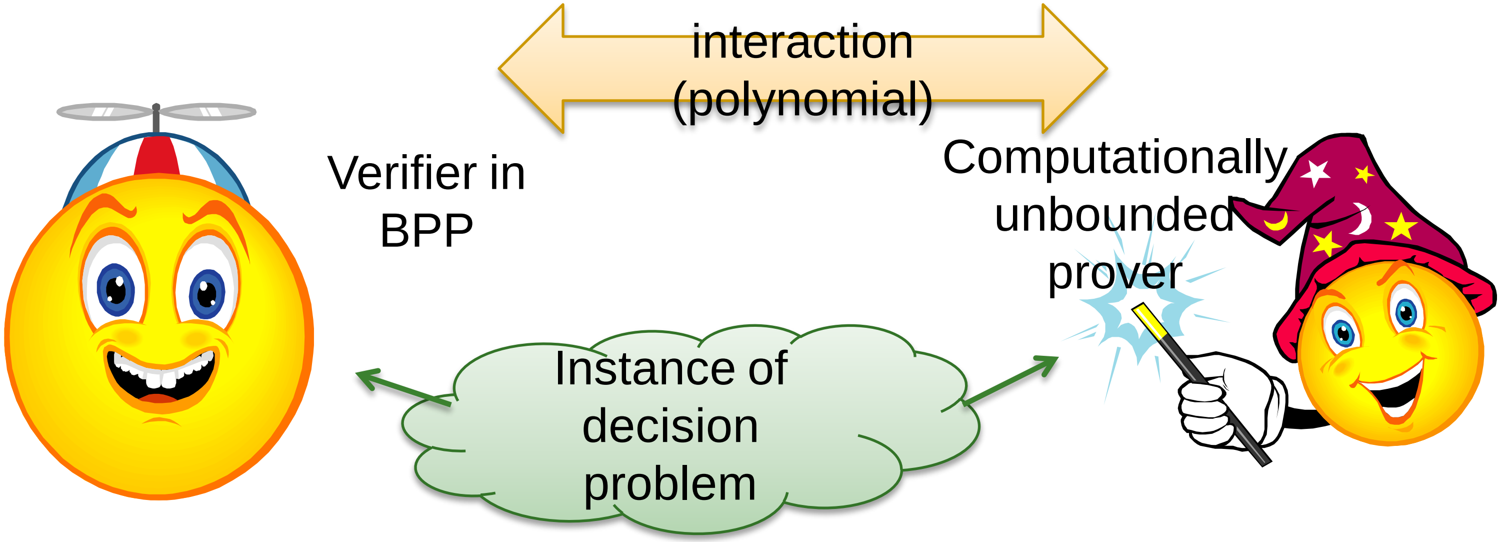
Interactive Proofs

Cryptography

Interactive proofs

...how useful is a cheating oracle?

Classical interactive proofs (**IP**)



interaction
(polynomial)

Verifier in
BPP

Computationally
unbounded
prover

Instance of
decision
problem

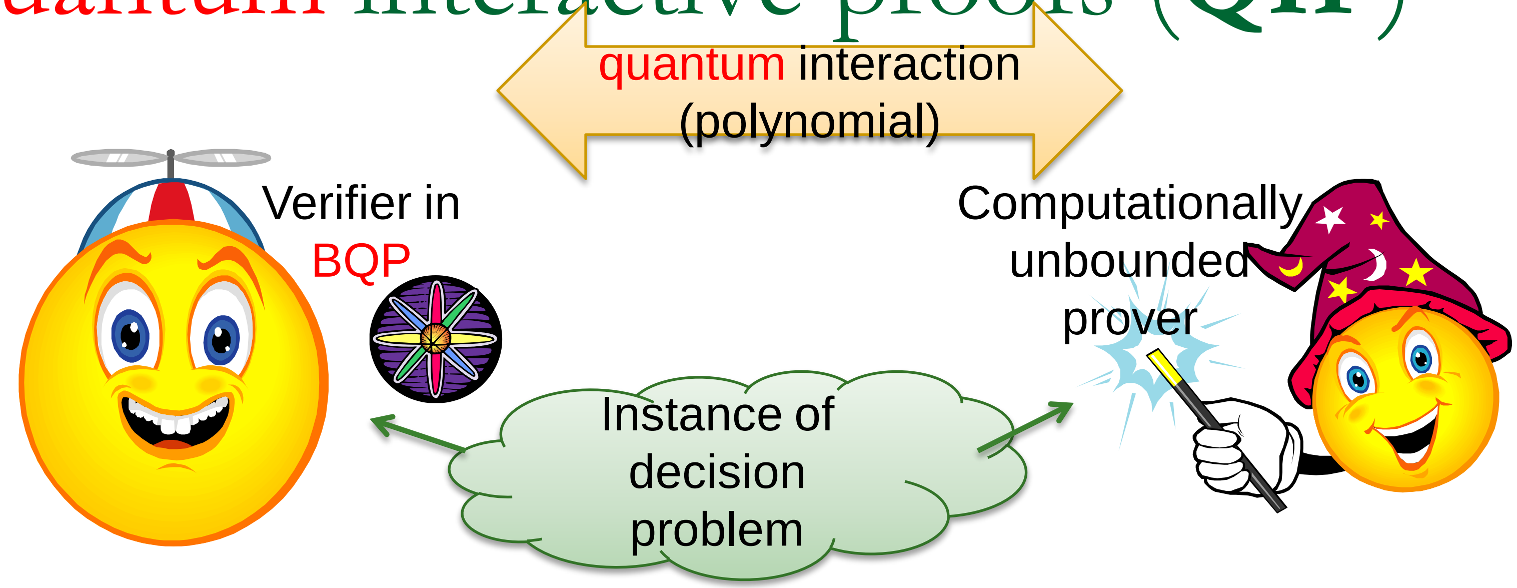
A language **L** is in **IP** if there exists a verifier such that:

•If the answer is "yes“, the prover must be able to behave in such a way that the verifier accepts with probability at least 2/3

•If the answer is "no“, then however the prover behaves, the verifier must reject with probability at least 2/3.

IP = **PSPACE** (Shamir, Lund-Fortnow-Karloff-Nisan 1990)

Quantum interactive proofs (**QIP**)



quantum interaction (polynomial)

Verifier in BQP

Computationally unbounded prover

Instance of decision problem

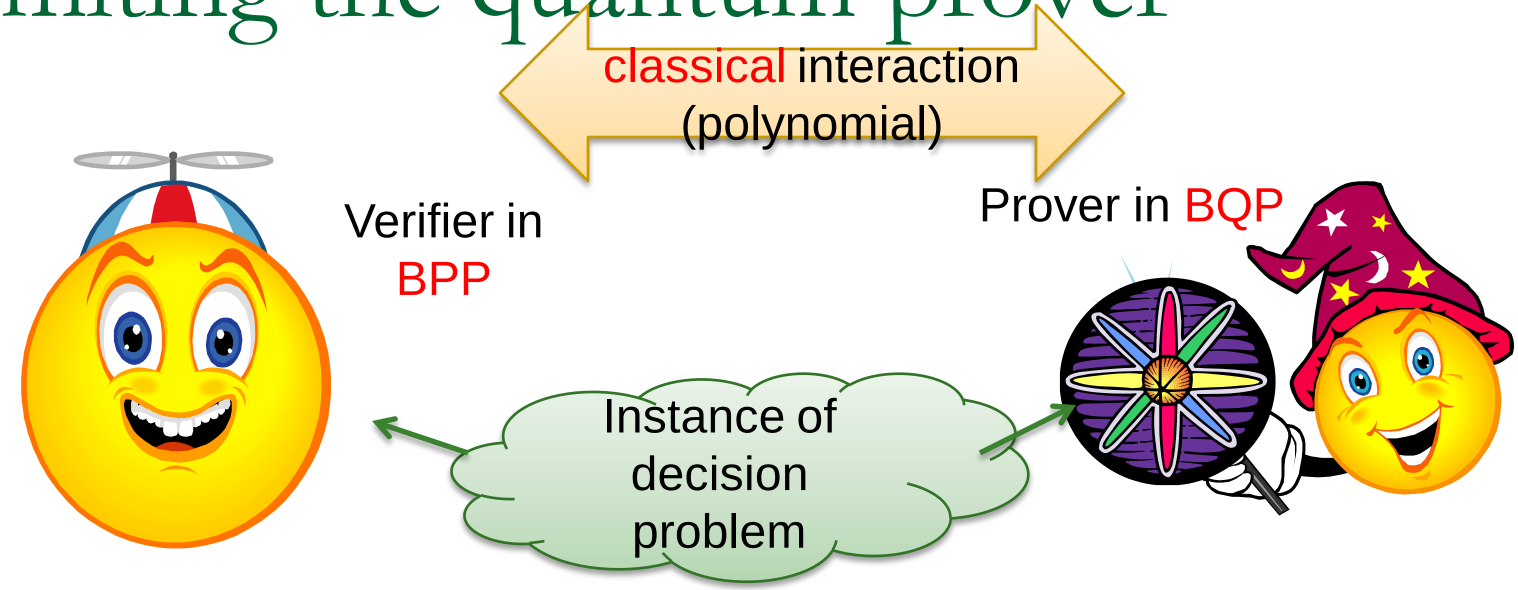
A language **L** is in **QIP** if there exists a verifier such that:

- If the answer is "yes," the prover must be able to behave in such a way that the verifier accepts with probability at least 2/3
- If the answer is "no," then however the prover behaves the verifier must reject with probability at least 2/3.

- **PSPACE** is in **QIP[3]** (Watrous 1999)
- **QIP[k]** = **QIP[3]** = **QIP** (k >= 3) (Kitaev-Watrous 2000).

- Open question: Does **QIP** strictly contain **IP** (i.e. does quantum computation add any power to interactive proofs?)

Limiting the quantum prover



classical interaction (polynomial)

Verifier in BPP

Prover in BQP

Instance of decision problem

- Open question: what is the power of this type of scenario?

$$\mathrm{IP}_{\mathbf{BQP}} \overset{?}{=} \mathrm{BQP}$$

- Our contribution: we give solutions to closely related problems:

1. Almost-classical verifier (has the additional power of generating random qubits from a fixed finite set):

$$\mathrm{IP}^{|\theta\rangle}_{\mathbf{BQP}} = \mathrm{BQP}$$

2. Purely classical verifier, with two BQP provers that cannot communicate but that share entanglement

$$\mathrm{MIP}^{*}_{\mathbf{BQP}} = \mathrm{BQP}$$

Major open problem: characterize the power of MIP*.

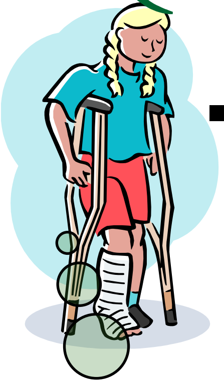
Cryptography

...what can be accomplished in the presence of an adversary?

Cryptography

- Quantum key distribution (QKD) (Bennett-Brassard 1984)
- Impossibility of Bit Commitment (Mayers, Lo-Chau 1995)
- Private Quantum Channels (Ambainis-Mosca-Tapp-de Wolf 2000)
- Quantum Authentication (Barnum-Crépeau-Gottesman-Smith-Tapp 2002)
- Multi-party computation (Ben-Or-Crépeau-Gottesman-Hassidim-Smith 2006)
- Cryptography in the bounded quantum-storage model (Damgard-Fehr-Salvail-Schaffner 2005)

Blind Quantum Computing



I have a classical computer and very limited quantum power

I have a quantum computer

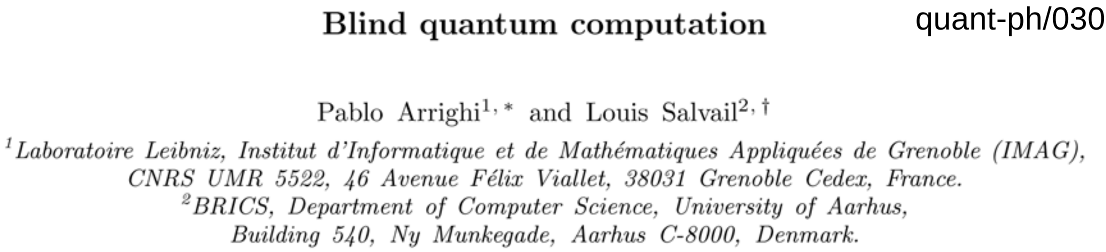
Our protocol achieves perfect privacy & detection of interfering Bob;

It can also be used for quantum inputs or outputs

Motivations

- Factoring
  - Using Shor's algorithm, Alice can use Bob to help her factor an integer corresponding to an RSA public key
    - Bob won't learn whose private key he is breaking; in fact he won't even know that he is helping Alice factor.
- BQP-Complete problem
  - No known efficient method to verify solution: we therefore give a method to authenticate Bob's computation.
- Processing quantum information
  - Blind state preparation, blind measurement…

Previous work



Blind quantum computation

Pablo Arrighi[1,*] and Louis Salvail[2,†]

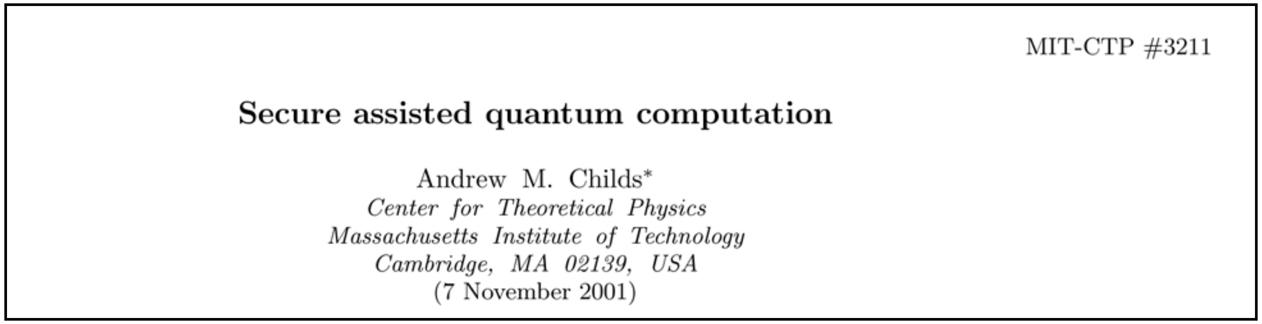
[1] *Laboratoire Leibniz, Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG),*
CNRS UMR 5522, 46 Avenue Félix Viallet, 38031 Grenoble Cedex, France.
[2] *BRICS, Department of Computer Science, University of Aarhus,*
Building 540, Ny Munkegade, Aarhus C-8000, Denmark.

quant-ph/0309152

- Publicly-known classical random-verifiable function
- Alice needs to be able to prepare and measure multi-qubit states
- Provides only *cheat sensititivity*

Previous work

arXiv:quant-ph/0111046



MIT-CTP #3211

Secure assisted quantum computation

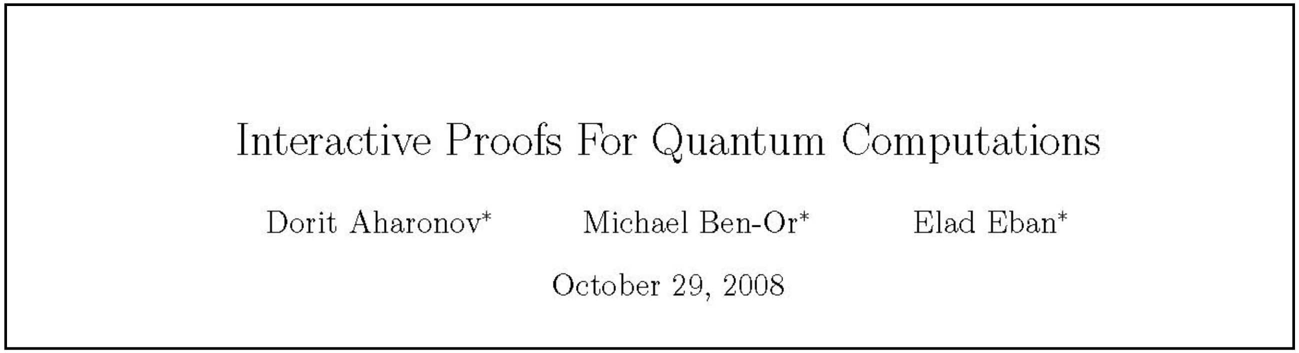
Andrew M. Childs*
Center for Theoretical Physics
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
(7 November 2001)

- Alice needs a quantum memory, and the ability to perform Pauli gates $X=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Idea: she sends encrypted qubits to Bob who applies a known gate. Alice can decrypt the qubits while preserving the action of the gate. Repeat, cycling through universal set of gates.

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pi/8=\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}, CNOT=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Concurrent work

arXiv:0810.5375



Interactive Proofs For Quantum Computations

Dorit Aharonov* Michael Ben-Or* Elad Eban*

October 29, 2008

- Interactive proof with BQP prover, and nearly-classical verifier.
  - Verifier has a constant-size quantum computer
  - Protocol is also *blind*.

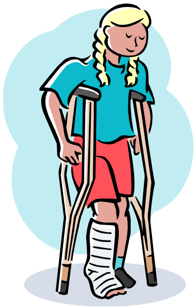
Our solution

Blind protocols that show:

$$\mathsf{BQP} = \mathsf{IP}^{|\theta\rangle}_{\mathsf{BQP}}$$

$$\mathsf{BQP} = \mathsf{MIP}^{*}_{\mathsf{BQP}}$$

High-level protocol



Classical input, classical output

Input built into circuit

- prepares qubits randomly chosen in

$$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{4}, n = 0, 1, \ldots, 7\}\}$$

$|\uparrow\rangle$ $|\searrow\rangle$ $|\leftarrow\rangle$ $|\swarrow\rangle$

$|\uparrow\rangle$ $|\rightarrow\rangle$ $|\swarrow\rangle$ $|\leftarrow\rangle$

$|\nearrow\rangle$ $|\nearrow\rangle$ $|\uparrow\rangle$ $|\rightarrow\rangle$

repeat $\left\{ \right.$

- Classical computation

Classical Communication

- Applies quantum operations and measurements

- Alice gets the output

Our technique

- Derived from Measurement Based quantum computing (MBQC)

  [Raussendorf and Briegel, 2001]
- First time that a new functionality is achieved in MBQC.

The MBQC paradigm

Qubits are measured layer-by-layer…

How to convert any quantum circuit to MBQC:

1. Start with *cluster state*
2. Perform $\{|0\rangle, |1\rangle\}$-basis measurements, depending on position of CNOT gates in quantum circuit
3. Perform x-y plane measure adaptively, layer by layer

Final layer is output

Each qubit *j* ha target measureme gle ϕ_j

qubit in

$|1\rangle$

…
ada

Each edge a two-qubit interaction

$$C-Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\phi'_j = (-1)^{s_x^j}\phi_j + \pi s_z^j$$

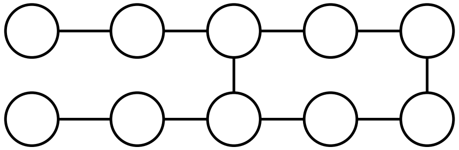
$(s_x^j \in \{0,1\}$ **and** $s_z^j \in \{0,1\}$ **depend on previous measurement outcomes)**

Measure in basis

$$\{\tfrac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_j}|1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - e^{i\phi_j}|1\rangle)\}$$

Getting rid of $\{|0\rangle,|1\rangle\}$ -basis measurements

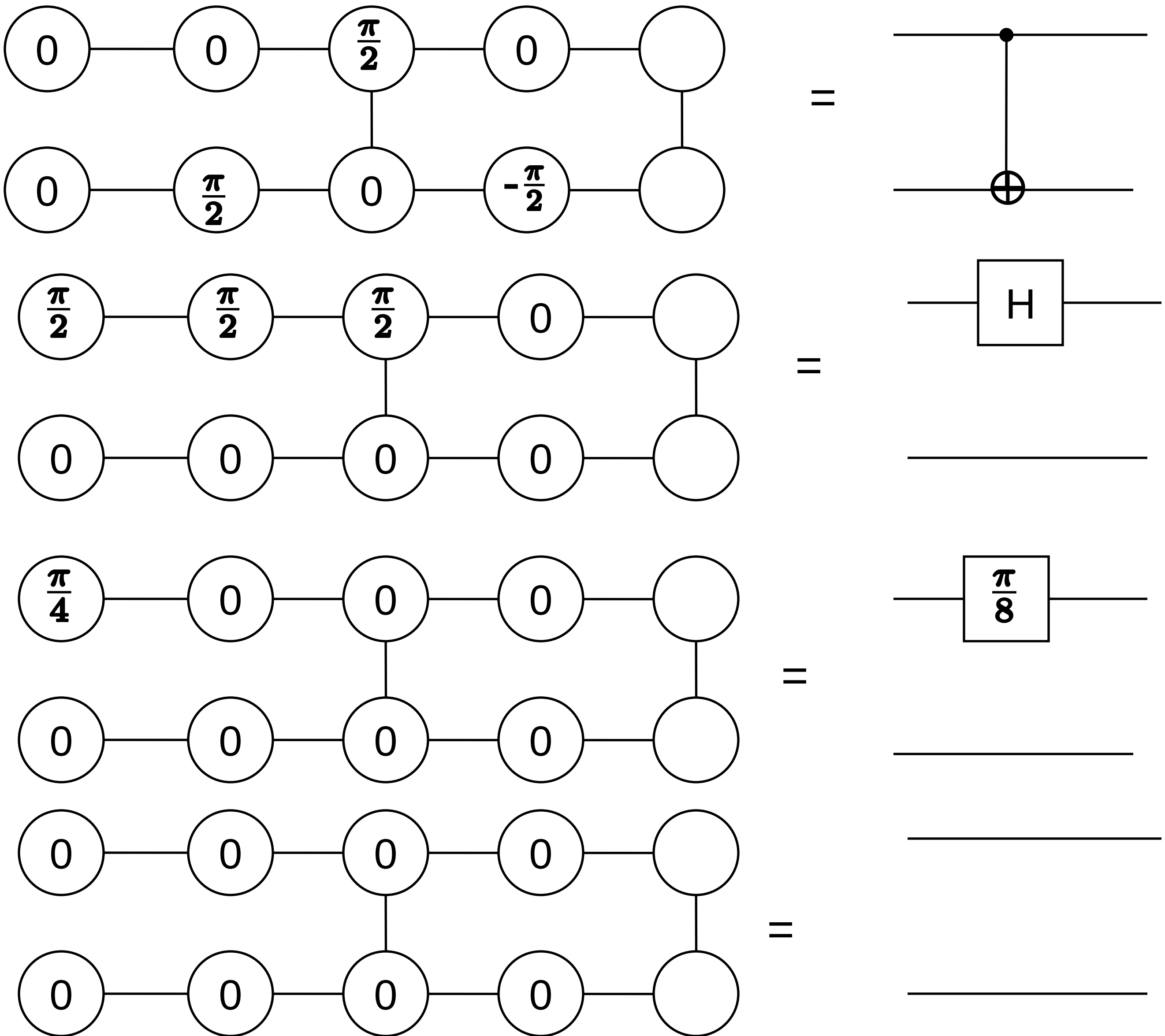
- We want to get rid of computational basis measurements that reveal the structure of underlying circuit
- We'll show that



yields universal set of gates: CNOT, H, and π/8

- Tilling the 2-qubit gate allows multiple inputs and multiple gates

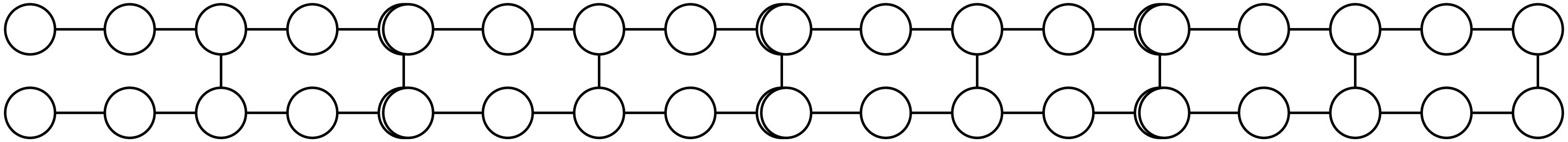
Getting rid of $\{|0\rangle,|1\rangle\}$ -basis measurements



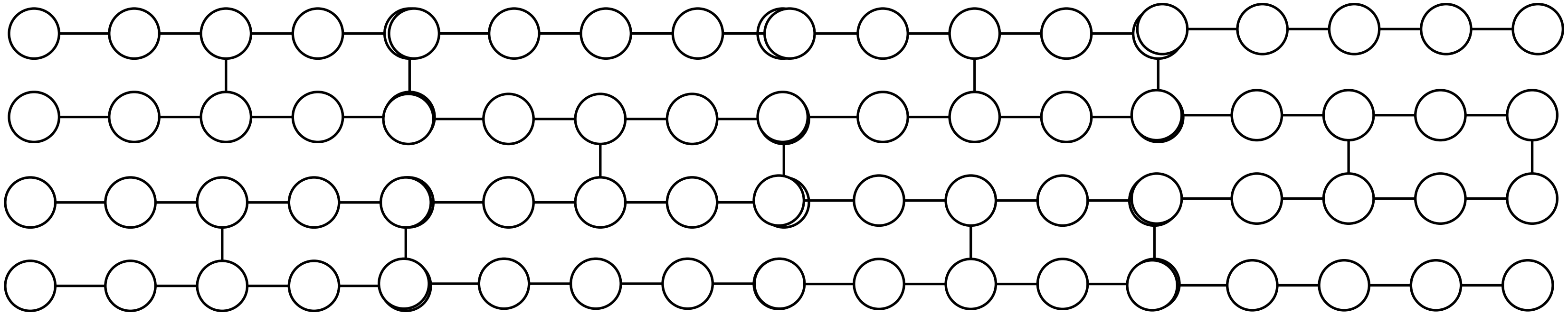
Getting rid of $\{|0\rangle, |1\rangle\}$ -basis measurements

The *brickwork* states

2-qubit circuit



4-qubit circuit



n-qubit circuit…

All measurements are integer multiples of $\frac{\pi}{4}$.

Blin ol

Alice's Z-rotation..

...commutes with Bob's control-Z.

- prepares qubits randomly chosen in

$$\{\tfrac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\tfrac{n\pi}{4}, n = 0,1,\ldots,7\}\}$$

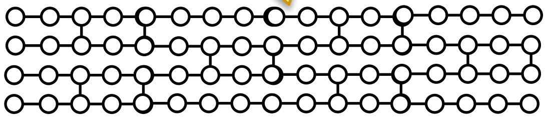
|↖⟩ |↘⟩ |←⟩ |↙⟩

|↑⟩ |→⟩ |↙⟩ |←⟩

|↗⟩ |↗⟩ |↑⟩ |→⟩

→

- entang ccording to **brickwor** state



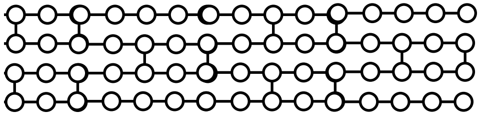
Measuring in δ basis cancels out Z-rotation

- chooses x-y pla measurement angles, adaptiv , layer by layer

$$\xrightarrow{\delta_1,\delta_2,\delta_3,\delta_4}$$

- single-qubit measurements in basis

$$\{\tfrac{1}{\sqrt{2}}(|0\rangle + e^{i\delta}|1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - e^{i\delta}|1\rangle)\}$$



$$\delta = \phi' + \theta + \pi r$$

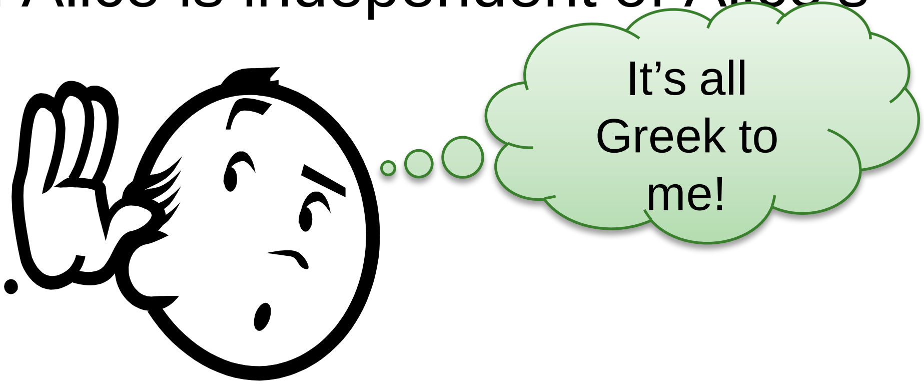
$$\phi' = (-1)^{s_x}\phi + \pi s_z$$

r random. r=1 flips Bob's measurement outcome. Alice can correct this.

Privacy

- Intuitively, we want that from Bob’s point of view, all information received from Alice is independent of Alice’s input **X**.

$\pi\kappa\ \Omega\alpha\beta\delta\psi\phi\delta\ldots$



- Bob does learn the dimensions of the brickwork state, giving an upper bound on the size of Alice's computation. He may also have some prior knowledge on **X**.
- Hence, we need to prove that Bob's view of the protocol does not depend on **X**, given his prior knowledge.

Privacy

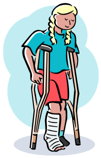
- Formally:

  We say that a protocol is *blind while leaking at most **L(X)*** if for any fixed **Y=L(X)**, the following two hold when given **Y**:

  1. The distribution of the classical information obtained by Bob is independent of **X**.
  2. The state of the quantum system obtained by Bob is fixed and independent both of **X** and of the distribution of the classical information above.

- Theorem: Our protocol is blind, while leaking at most the dimensions of the brickwork state.

Privacy



- prepares qubits randomly chosen

$\{\frac{1}{\sqrt{2}}(|0\rangle$ $e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{4}, n = 0, 1, \ldots, 7\}\}$

Let $\theta' = \theta + \pi r$ and $\vec{\theta'} = (\theta'_1, \theta'_2, \theta'_3, \ldots)$

- chooses x-y plane measurement angles, adaptive layer by layer

$$\delta = \phi' + \theta + \pi r$$

$$\phi' = (-1)^{s_x}\phi + \pi s_z$$

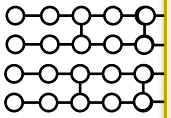
Let **A** be the quantum system initially sent from Alice to Bob

Let $\vec{\delta} = (\delta_1, \delta_2, \delta_3, \ldots)$ be the classical information that Bob gets during the protocol

Hence $\vec{\delta} = \vec{\phi'} + \vec{\theta'}$

$\vec{\theta'}$ is random, so $\vec{\delta}$ and $\vec{\phi}$ are independent

- entan **brick**



gle

bas

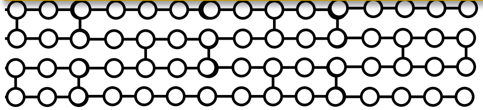
$\{\frac{1}{\sqrt{}}$

Fix $\vec{\delta}$. Because **r**’s are random, for each qubit of **A**, one of the following two has occurred:

$$r = 0 \text{ so } |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\delta-\phi')})|1\rangle.$$

$$r = 1 \text{ so } |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\delta-\phi)})|1\rangle.$$

Hence when **r** is unknown, **A** consists of copies of the two-dimensional completely mixed state, which is fixed and independent of $\vec{\phi}$.



Detecting an interfering Bob

For classical outputs that cannot easily be verified

  - Double the number of wires, randomly adding N/2 wires in $|0\rangle$ and N/2 wires in $|1\rangle$.
  - An actively interfering Bob is caught with probability at least ½. Repeat s times.
- We also have a fault-tolerant version that additionally provides authentication for quantum inputs and outputs.

Interactive proof

Verifier in BPP + random qubits

interaction

Prover in BQP

- The blind protocol is as an interactive proof for any problem in BQP.

It follows:

$$\mathsf{BQP} \subseteq \mathsf{IP}^{|\theta\rangle}_{\mathsf{BQP}}$$

Trivially,

$$\mathsf{BQP} \supseteq \mathsf{IP}^{|\theta\rangle}_{\mathsf{BQP}}$$

Hence,

$$\mathsf{BQP} = \mathsf{IP}^{|\theta\rangle}_{\mathsf{BQP}}$$

Multi-prover interactive proofs

$\tilde{\theta}_1, \tilde{\theta}_2, \ldots$

Cheating is detected by the authentication procotol

$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\tilde{\theta}_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\tilde{\theta}_j}|1\rangle)\}$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)^{\otimes N}$$

Classical part of blind QC using

$$\theta_j = \tilde{\theta}_j + m_j\pi$$

Our result:

$\mathsf{BQP} \subseteq \mathsf{MIP}^*_{\mathsf{BQP}}$

Trivially,

$\mathsf{BQP} \supseteq \mathsf{MIP}^*_{\mathsf{BQP}}$

Hence, $\mathsf{BQP} = \mathsf{MIP}^*_{\mathsf{BQP}}$

Open questions

- Is quantum communication required for blind quantum computation?
- $$\mathrm{IP}_{\mathrm{BQP}} \overset{?}{=} \mathrm{BQP}$$

Thank you